Remarks

Claims 1-26 are pending in the application. All claims stand rejected by the Office Action dated July 13, 2005. By this paper claims 1, 15, 21, and 26 have been amended. Claims 1-4, 7, and 9-26 are rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. App. No. 2004/0264435 to Chari et al. (Chari) in view of U.S. Pat. No. 6,546,493 to Magdych et al. (Magdych). Claims 5-6, and 8 are rejected under 35 U.S.C. § 103(a) as being unpatentable further in view of U.S. Pat. App. No. 2001/0047401 to Moore et al. (Moore).

Claim Rejections

Independent claims 1, 15, 21 and 26 are rejected in the Office Action under 35 U.S.C. § 103(a) as unpatentable over Chari in view of Magdych. In order to advance prosecution, these claims have been amended to clarify that when a network device is first connected to a network, a scanning module remotely and automatically scans the network device. See application, p. 11, ¶ 35. Automatically is without human intervention and is thus performed without action by a user. As amended, claim 1 recites a method for scanning network devices connected to a network, comprising:

> (a) detecting connection of a first network device to the network; and
> (b) performing remote agentless scanning of the first network device automatically in response to detection of the first network device.

Claims 15, 21, and 26 have been amended similarly.

BEST AVAILABLE COPY

PAGE 10/16 * RCVD AT 10/13/2005 7:00:29 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-18

Chari and Magdych Do not Teach or Suggest Automatic Scanning "In Response To" Detection of a Network Device

The Office Action concedes that Chari does not teach scanning of the first network device in response to detection of the first network device. Magdych teaches the use of either a risk assessment scanning tool or an intrusion detection tool. Magdych teaches that risk assessments and intrusion detection is through passive monitoring of network communication. This is true despite probing of the network (discussed later). Once an "anomaly" (i.e. an attack, intrusion, or possible virus activity) is detected, then action is taken in the form of remedies. Magdych, col. 3, lines 22-67. Nowhere in Magdych is there disclosed or suggested an automatic scanning of a newly detected network device regardless of currently present vulnerabilities.

Magdych's Figure 3 is a flowchart of the method for detecting intrusions to a network, which together with its accompanying disclosure, further solidifies use of passive monitoring:

> In operation 304, network communications are monitored . . . packet-by-packet. It is then determined whether the currently (sic) network communications exploit a known vulnerability or violate a policy in decision 308. ... If it is found that the network communications exploit a known vulnerability or violate a policy in decision 308, a remedying event is executed.

Magdych, col. 5, lines 8-20. Thus, Magdych requires perception of an anomalous event in network communications prior to taking remedial action. No mention is made of the network device or automatic scanning of the network device.

BEST AVAILABLE COPY

PAGE 11/16 * RCVD AT 10/13/2005 7:00:29 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-18

Specifically, the risk assessment tool may "probe for network weaknesses by simulating certain types of security events that make up and attack." Id., col. 3, lines 26-28. Likewise, the intrusion detection tool:

> detects attacks or intrusions by scanning network communications between the various foregoing network devices. . .This scanning may include comparing the network communications, etc. with a plurality of virus/attack signatures, known vulnerabilities and/or policies that may be constantly updated.

Id., col. 3, lines 36-44. Upon detection of an attack, break of policy, or other anomaly, a list of possible remedies are considered. Id. col. 3, lines 44-49.

In contrast, claims 1, 15, 21 and 26 all claim that the scanning is of the network device itself and that the agentless remote scan happens "automatically in response to detection of the first network device." After detection of the network device, a vulnerability scan is automatically executed directly on the network device to ensure that it is not introducing any security risks and/or viruses, etc., into the network. This automatic scan has the advantage of catching and fixing vulnerabilities or virus risks before the first network device has an opportunity to interact on the network and release them. So-called "time-bomb" viruses, for instance, can be scanned for and eliminated on the network device before it has a chance to be set off to infect the rest of the network.

Magdych, however, would wait until an "anomaly" or other security risk is detected in the communication over the network, perhaps in response to a network probe simulating an attack. Then, only upon detecting the communicated anomaly would it decide whether remedial action should be taken. Magdych's passive listening (or "network scanning") would allow a "time-bomb" virus to be first set off

BEST AVAILABLE COPY

PAGE 12/16 * RCVD AT 10/13/2005 7:00:29 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-18

and to begin replicating across a network (thus being detected) before action would be taken. This would be especially true in communication monitoring mechanisms having latencies of differing lengths. A remedy such as quarantine may thus be too late, and disinfecting the network of the virus may be very difficult, if not impossible, if the virus was fast enough in its replication and infection of other network devices before detection.

Applicant also discloses that the scanning module may further include a security policy management module so that security and compliance policies are immediately complied with and so that future compliance updates may be scheduled. See Fig. 3 and accompanying disclosure. Here, the application emphasizes the active role of getting into any newly detected network device and actively updating and insuring its compliance to prevent current and future virus outbreaks or exploitations of vulnerabilities.

Specifically, the "setting policy" stage allows a network server to automatically set policies upon scanning when the device is first detected. The "audit" stage may also take place upon an initial scan as well as at future scheduled times, taking data off the device to:

> identify missing patches and identify unauthorized software (e.g., software with back doors), delete unlicensed or unauthorized software, identify unauthorized hardware [ ], eliminated unused system administration passwords on distributed systems, and/or provide control of external auditor's rights and responsibilities.

Application, p. 15, ¶ 47-48. Thus, this part of applicant's disclosure is in harmony with "performing remote agentless scanning of the first network device automatically in response to detection of the first network device." Nowhere in

BEST AVAILABLE COPY

PAGE 13/16 * RCVD AT 10/13/2005 7:00:29 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-18

Chari or Magdych is this limitation from applicant's independent claims either claimed or suggested.

"To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art." MPEP § 2143.03. Because neither Chari nor Magdych teaches or suggests, alone or in combination, all the elements of claims 1, applicant respectfully submits that these references do not render claim 1 unpatentable. Applicant further respectfully submits that claims 15, 21, and 26, with similar amendments, are patentably distinct over the cited references for at least the above argued reasons. Claims 2-14, 16-20, and 22-25 are also patentably distinct by virtue of their dependence from claims 1, 15, and 21, respectively.

Chari and Magdych Do Not Teach or Suggest "Determining Items to Scan Based on At Least One" Property

The Office Action rejected claim 21 as unpatentable under 35 U.S.C. § 103(a) over Chari in view of Magdych based on the above-discussed language present in claim 1, in addition to further language purported to be taught by Magdych. This language in claim 21 reads: "determining items to scan based on at least one of the properties." "The properties" is referring to properties "associated with the first network device to determine the identity of the first network device." Identifying the first network device is one way to detect the device's initial connection to the network.

The Office Action concedes the limitations of "(d) determining items to scan based on at least one of the properties; and (e) performing remote scanning of the first network device in response to the determination of the connection of the first

BEST AVAILABLE COPY

network device to the network." Magdych does not disclose the detection of a first network device and neither does Magdych teach the identifying of properties associated with identifying a first network device. In so concluding, Magdych cannot disclose "determining items to scan based on at least one of the properties".

Magdych teaches the passive monitoring of network communications to find "anomalies," and thus vulnerabilities or security threats. In response thereto, Magdych may, in addition to other remedies, conduct a risk assessment scan of those devices found to be the source of the anomalies. Col. 5, lines 18-25. In other words, Magdych's scanning is not triggered by first detecting a device based on certain ascertained properties it has, but by finding a vulnerability or anomaly first. Then Magdych teaches subsequently seeking out the device source of the vulnerability or anomaly to then scan. See Magdych, col. 4, lines 3-9.

Claim 21's querying and determining steps focus on a specific network device by locating data on a server about the device. The method of claim 21 determines items to be scanned based on at least one property. Magdych does not teach or suggest "determining items to scan based on at least one of the properties".

Because Chari and Magdych do not teach or suggest all the elements of claim 21, alone or in combination, claim 21 represents patentable subject matter. Also, for these further reasons, claims 22-25 are likewise patentably distinct by virtue of their dependency on claim 21.

Reconsideration of all pending claims in view of the amendments and following remarks is respectfully requested.

BEST AVAILABLE COPY

PAGE 15/16 * RCVD AT 10/13/2005 7:00:29 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-18

Respectfully submitted,

Altiris, Inc.

By _____
John R. Thompson
Registration No. 40,842

STOEL RIVES LLP
One Utah Center Suite 1100
201 S Main Street
Salt Lake City, UT 84111-4904
Telephone: (801) 328-3131
Facsimile: (801) 578-6999

BEST AVAILABLE COPY

PAGE 16/16 * RCVD AT 10/13/2005 7:00:29 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/28 * DNIS:2738300 * CSID:801 578 6999 * DURATION (mm-ss):03-18